Information Security Policy Statement of Intent

I, Charles Aris, Chief Executive Officer of Tower Supplies, recognise that the security of our employees, contractors, visitors and interested parties' information is of the utmost importance and fundamental to our business.

We are committed to ensuring, so far as is reasonably practicable, appropriate technical and organisational measures to protect information assets against loss, unauthorised access, misuse, alteration, or disclosure

Leadership & Responsibility

The overall responsibility for Information Security rests with me as CEO.

Responsibilities are shared across the organisation:

- Leaders and managers are responsible for implementing information security and managing risks within their areas
- Employees are expected to understand their individual responsibilities under information security, and follow the secure operating procedures as set out by Tower Supplies Leadership.

We will ensure that competent advice is available where necessary to support effective risk management.

Our Commitments

We will:

- Establish and maintain an Information Security Management System which satisfies the requirements of ISO 27001:2022, and all applicable statutory, regulatory and customer requirements.
- Implement and maintain controls to preserve the confidentiality, integrity, and availability of information.
- Manage information assets, ensuring they are identified, assessed and protected in accordance with their sensitivity, ownership and importance.
- Consult with our employees on issues relating to information security to foster a positive security culture.
- Restrict information access to authorised users in accordance with the principle of least privilege.
- Manage information security risks on an ongoing basis. Selecting and implementing suitable controls to reduce security risks to an acceptable level.
- Provide employees with appropriate information, instruction, training and supervision to recognise information security risks and fulfil their individual information security and data protection responsibilities.
- Establish effective arrangements to communicate the Management System to employees so that they are aware of their obligations, policies, and procedures, so it is understood and implemented by all employees.
- Promote a culture whereby employees are openly encouraged to report information security incidents, including near misses, without fear of reprisal, to ensure the root causes of incidents are identified to eliminate recurrence.
- Ensure adequate financial, technical and physical resources are available to meet the objectives of the Information Security Management System.
- Ensure supplier and third-party information security risks are identified and managed through appropriate contractual and assurance mechanisms.

Our Approach

We are committed to preventing security incidents and creating an environment where security is considered in all business decisions.

We will review our performance, learn from experience, and continually improve our Information Security Management System.

Review

This policy will be reviewed at least annually, or sooner where significant changes occur.

Charles Aris
Chief Executive Officer

Date: 20th May 2026